UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MATTHEW WEISS,	:	
Plaintiff,	:	**MEMORANDUM DECISION AND ORDER**
- against -	:	
	:	20-cv-1460 (BMC)
EQUIFAX, INC. and EQUIFAX INFORMATION SERVICES, LLC,	:	
Defendants,	:	

COGAN, District Judge.

Plaintiff brings this action for alleged violations of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.*; the New York FCRA, N.Y. Gen. Bus. Law § 380 *et seq.*; and N.Y. G.B.L. § 349. He alleges that defendants failed to correct inaccurate information in his credit report and falsely led him to believe they would safeguard his personal data from hackers. Before me is defendants' motion to dismiss the complaint under Fed. R. Civ. P. 12(b)(6) on three grounds: (1) Counts I and IV fail to state a claim because the complaint is devoid of facts concerning defendants' investigation or procedures; (2) the data breach claim in Counts II and VI are not actionable under the FCRA and N.Y. G.B.L. § 349, respectively; and (3) alternatively, these latter claims are barred because plaintiff failed to timely opt out of a class action settlement resolving all claims arising from the data breach.[1]

The motion is granted in part and denied in part. Maintaining reasonable procedures is an affirmative defense under the FCRA, and thus plaintiff was not required to anticipate and negate

[1] Plaintiff has withdrawn Counts III and V.

this defense in his pleading. Furthermore, the data breach allegations alleged under N.Y. G.B.L. § 349 state a plausible claim and, because the complaint alleges that plaintiff opted out of the class action settlement, that claim may proceed. However, the FCRA claim based on the data breach fails to state a claim and is therefore dismissed.

SUMMARY OF COMPLAINT

In 2017, foreign hackers invaded defendants' computer systems and stole the sensitive personal data of over 145 million consumers. Plaintiff was one such identity theft victim, and multiple fraudulent credit and checking accounts were later opened in his name.

To limit the data breach's impact on his credit score, plaintiff filed a police report and obtained an Identity Theft Report from the Federal Trade Commission. He then notified his creditors and multiple consumer reporting agencies, including defendants, that identity thieves had fraudulently opened various accounts under his name, also sending them copies of the police and FTC reports. Despite plaintiff's numerous efforts to have these bogus accounts removed from his credit report, defendants failed to delete this disputed information.[2]

Rather than removing the fraudulent accounts from plaintiff's credit report, defendants deleted the wrong information, namely, his correctly reported accounts with Credit One and P.C. Richard & Son, Inc. Because of defendants' failures, plaintiff could not obtain a new credit card or open a checking account, and his credit score decreased, which forced him to pay a higher rate of interest on the loans he was able to secure.

Based on the hack and resulting data breach, hundreds of cases were filed nationwide and consolidated as a multidistrict litigation proceeding ("MDL") in the Northern District of Georgia. See In re Equifax Customer Data Security Breach Litigation, No. 17-md-2800 (N.D. Ga.).

[2] The other CRAs accepted plaintiff's protest and deleted the disputed information.

Defendants and the named plaintiffs in that case eventually entered into a class action settlement agreement. Excluded from the settlement class were individuals who executed timely and valid requests to opt out. According to the complaint, "Plaintiff opted out of the nationwide class action concerning the hack."

Plaintiff's complaint contains four remaining claims for relief: (1) defendants willfully or negligently violated 15 U.S.C. § 1681e(b) and 1681i by failing to follow reasonable procedures to assure the accuracy of his credit report and by failing to conduct a reasonable investigation, respectively (Count I); (2) defendants prepared an erroneous credit report in violation of the New York FCRA and failed to assure maximum accuracy of the credit report when they failed to conduct a reasonable investigation as to plaintiff's disputes (Count IV); (3) by failing to prevent the data breach, defendants willfully or recklessly violated their legal obligations under the FCRA (Count II); and (4) defendants violated N.Y. G.B.L. § 349 when they, among others things, failed to implement security and privacy measures to safeguard plaintiff's sensitive information and misrepresented to him that his personal data would be protected from outside threats (Count VI).

DISCUSSION

I. Standard of Review

Under Federal Rule of Civil Procedure 8(a)(2), a complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Thus, to survive a motion to dismiss under Rule 12(b)(6), a complaint must include "enough facts to state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). "Factual allegations must be enough to raise a right to relief above the speculative level." Id. at

555. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

The purpose of the FCRA is "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer[.]" 15 U.S.C. § 1681(b). Specifically, the FCRA requires that consumer reporting agencies ("CRAs") "follow reasonable procedures to assure maximum possible accuracy of the information" contained in the consumer report. 15 U.S.C. § 1681e(b). To succeed on a claim under Section 1681e(b), a plaintiff must show that:

> (1) the [CRA] was negligent [or willful] in that it failed to follow reasonable procedures to assure the accuracy of its credit report; (2) the consumer reporting agency reported inaccurate information about the plaintiff; (3) the plaintiff was injured; and (4) the [CRA's] negligence proximately caused the plaintiff's injury.

Whelan v. Trans Union Credit Reporting Agency, 862 F. Supp. 824, 829 (E.D.N.Y. 1994).

When a report's accuracy is disputed, Section 1681i outlines specific procedures that CRAs must follow to ensure the proper reinvestigation of the disputed information. 15 U.S.C. § 1681i. This includes reinvestigating a consumer's record within a reasonable period of time after the consumer raises the issue with the CRA. Id. What constitutes a "reasonable" reinvestigation depends on the circumstances. Jones v. Experian Info. Solutions, Inc., 982 F. Supp. 2d 268, 273 (S.D.N.Y. 2013).

II. Defendants' Procedures

I reject defendants' argument that, because plaintiff failed to allege facts as to defendants' procedures, the complaint fails to state claim. First, as a practical matter, a consumer understandably has little information as to the internal processes a CRA has implemented to ensure maximum accuracy of one's credit report. After lodging a dispute, a consumer, in most

cases, will simply receive a form letter from the CRA, stating it has investigated the issue and determined that no adjustment is necessary. Only defendants can provide the facts showing the reasonableness behind their actions in response to plaintiff's dispute letter.

It follows from this that by challenging the complaint's lack of factual assertions as to their procedures, defendants are essentially raising a "reasonable procedures" defense. Although the Second Circuit has not addressed this issue, the courts that have expressly considered it hold that such an argument is an affirmative defense under the FCRA. See, e.g., Ricketson v. Experian Info. Solutions, Inc., 266 F. Supp. 3d 1083, 1093 (W.D. Mich. 2017); Taylor v. First Advantage Background Servs. Corp, 207 F. Supp. 3d 1095, 1106 (N.D. Cal. 2016); Action v. Bank One Corp., 293 F. Supp. 2d 1092, 1099 (D. Ariz. 2003); Thomas v. Trans Union, LLC., 197 F. Supp. 2d 1233 (D. Or. 2002). Plaintiff was not required to anticipate and negate an affirmative defense in his pleading. See Perry v. Merit Sys. Prot. Bd., 137 S. Ct. 1975, 1986 n.9 (2017).[3]

Here, plaintiff has alleged sufficients facts to state a plausible violation of 15 U.S.C. § 1681e(b) and 1681i. As described above, the complaint alleges that plaintiff repeatedly notified defendants that he was the victim of a hack targeting their computer systems; sent defendants reports corroborating his status as an identity theft victim; and that defendants removed perfectly accurate account information instead of the inaccurate information about which plaintiff was complaining. If defendants want to contend that this was the result of reasonable procedures, they are going to have to prove it. Accordingly, Counts I and IV may proceed.[4]

[3] Defendants rely on Nguyen v. Ridgewood Sav. Bank, No. 14-cv1058, No. 14-cv-3464, No. 14-cv-3989, 2015 WL 2354308 (E.D.N.Y. May 15, 2015). That court never expressly considered the issue of whether reasonable procedures is an affirmative defense. It simply assumed that a plaintiff had to plead lack of reasonable procedures.

[4] The FCRA and New York FCRA are interpreted in the same manner. See Cohen v. Equifax Info. Services, LLC, No. 18-cv-6210, 2019 WL 2451293, at *1 n.1 (S.D.N.Y. April 17, 2019); Trikas v. Universal Card Servs. Corp., 351 F. Supp. 2d 37, 46 (E.D.N.Y. 2005).

III. Data breach and the FCRA

Plaintiff's contention that FCRA liability flows from the data breach (Count II) is deficient. The complaint vaguely asserts that defendants "recklessly breached [their] own legal obligations concerning data security under the FCRA" and "intentionally deprived plaintiff of his rights under the FCRA." These are conclusory allegations, and defendants have no way to discern which particluar "legal obligations" were breached or what "rights" under the FCRA they are accused of violating. Even under the liberal notice pleading requirements, these allegations are inadequate. See Iqbal, 556 U.S. at 678.

In addition, courts have consistently held that a defendant's mere failure to safeguard personal data from hackers or thieves does not qualify as "furnishing" credit reports under the FCRA and thus cannot trigger liability under the statute. See, e.g., In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1313 (N.D. Ga. 2019); Galaria v. Nationwide Mut. Ins. Co., No. 13-cv-118, 2017 WL 4987663, at *4 (S.D. Ohio Aug. 16, 2017); Holmes v. Countrywide Fin. Corp., No. 5:08-cv-205-R, 2012 WL 2873892, at *16 (W.D. Ky. July 12, 2012). Nor is personally identifiable information stolen during a data breach a "consumer report" within the meaning of the FCRA. See, e.g., In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d at 1313–14; see also Parker v. Equifax Info. Servs., LLC, No. 15-cv-14365, 2017 WL 4003437, at *3 (E.D. Mich. Sept. 12, 2017) ("The accumulation of biographical information from Equifax's products does not constitute a consumer report because the information does not bear on Parker's credit worthiness.").

Accordingly, defendants' motion to dismiss Count II is granted.

IV. The Data breach and N.Y. G.B.L. § 349

On the other hand, plaintiff has stated a claim under N.Y. G.B.L. § 349 (Count VI) in relation to the data breach.[5] The complaint alleges that defendants (1) failed to implement security and privacy measures to protect plaintiff's sensitive and personal confidential information, (2) failed to identify obvious risks relating to the hack, (3) failed to safeguard plaintiff's sensitive and personal confidential information; (4) misrepresented to plaintiff that it would protect his information, (5) misled and concealed from him that defendants in fact did not secure his information from the risks pertaining to the hack, and (6) caused plaintiff to think that defendants were protecting his personal data.

Unlike the FCRA allegation arising from the data breach, which stems from defendants' inability to shield plaintiff's information from hackers, this claim for relief alleges that defendants' actions and representations caused plaintiff to think defendants were taking steps to protect his personal information, when in reality, they were not. This resulted in actual and pecuniary harm after plaintiff's identity was stolen and numerous unauthorized accounts were opened under his name. Defendants' motion to dismiss Count VI is denied.

V. MDL Settlement

Defendants cannot prevail on their final argument – that plaintiff failed to opt out of the MDL settlement. Defendants have annexed documents to their reply purporting to show that plaintiff submitted three claims to the MDL settlement administrator for compensation related to the data breach. If plaintiff in fact failed to execute a timely and valid request to opt out of the

[5] In Pelman ex rel. Pelman v. McDonald's Corp., 396 F.3d 508, 511 (2d Cir. 2005), the Second Circuit held that claims under § 349 are not subject to the heightened pleading standards of Rule 9(b).

settlement, then he is precluded from filing a new claim in any subsequent litigation, unless it is based on new facts that give rise to a new claim. See TechnoMarine SA v. Giftports, Inc., 758 F.3d 493 (2d Cir. 2014).[6]

In any event, plaintiff vehemently insists that he opted out of the data breach settlement and contends he is therefore not bound by the terms of the agreement. Even after defendants accused plaintiff of submitting claims to the MDL settlement administrator in their motion to dismiss, plaintiff doubled down in his opposition, reiterating that the complaint states that he opted out of the data breach settlement and arguing defendants are "bound" by his factual assertion in the complaint.

When deciding a motion to dismiss, I must accept as true all material factual allegations in the complaint, see J.S. ex rel. N.S. v. Attica Cent. Sch., 386 F.3d 107, 110 (2d Cir. 2004), and I am generally confined to the four corners of the complaint, documents attached to the complaint as exhibits, and any documents incorporated in the complaint by reference. See McCarthy v. Dun & Bradstreet Corp., 482 F.3d 184, 191 (2d Cir. 2007). Therefore, I must accept plaintiff's unambiguous statement contained in the complaint and disregard the extraneous documents submitted, for the first time, by defendants in their reply.

But plaintiff and his counsel are on notice. If it turns out that they are wrong and that plaintiff failed to execute a timely and valid request to be excluded from the class action settlement or otherwise received compensation from the MDL settlement, this likely would demonstrate bad faith on plaintiff's part and the lack of an adequate prefiling investigation by

[6] According to the MDL docket, the name "Matthew W." appears twice on the list of individuals who filed timely and valid exclusions to opt out of the settlement. See Dkt. No. [957], JND Identifier #1696 and 3730. Although the states of Hawaii and Arkansas are listed after these two names, respectively, and plaintiff's current domicile is New York, it is possible that plaintiff was one of these individuals. The matter will have to be resolved in discovery.

plaintiff's counsel. The consequences for such a fundamental failure are well established. See Fed. R. Civ. P. 11.

CONCLUSION

Defendants' [10] motion to dismiss is granted as to Count II and otherwise denied.

SO ORDERED.

Digitally signed by Brian M. Cogan

U.S.D.J.

Dated: Brooklyn, New York
July 7, 2020